PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-163379
(43)Date of publication of application : 16.06.2000

(51)Int.Cl. G06F 15/00
G01S 5/14
G06F 12/00
G06F 12/14
G09C 1/00
H04L 9/14

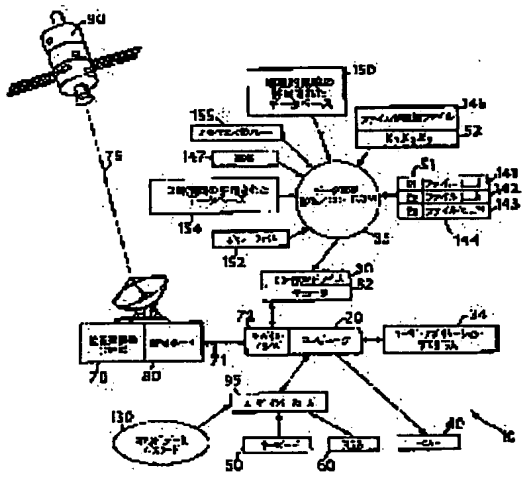
(21)Application number : 11-308358
(22)Date of filing : 29.10.1999

(71)Applicant : DATUM INC
(72)Inventor : HASTINGS THOMAS MARK
MCNEIL MICHAEL E
GLASSEY TODD S
WILLETT GERALD L

(30)Priority
Priority number : 98 182342 Priority date : 29.10.1998 Priority country : US

(54) CONTROL OVER ACCESS TO STORED INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To limit the use of information to a specified geographic area by determining the geographic position of stored information to be arranged according to a signal received by a receiver supplying position information and controlling access to the stored information.
SOLUTION: A GPS receiver 70 is arranged at the actual geographic position of a computer system 10 and receives a signal 75 from a circulating GPS satellite 90. According to the received data, the actual geometric position of information stored in a portable computer-readable CD-ROM used as a data distribution medium 35 is determined and the receiver 70 converts the received signal 75 geometric position data of precision of several meters as to the latitude and altitude and day/hour data 71 of precision of microseconds. Then the data 71 are passed through a device driver 72 to control access to stored information on the data distribution medium 35 through a CD-ROM drive 30.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－163379
（P2000－163379A）
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｄ
Ｇ０１Ｓ　5/14		Ｇ０１Ｓ	5/14	
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ	12/00	５３７Ａ
12/14	３１０		12/14	３１０Ｋ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ

審査請求　未請求　請求項の数28　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平11－308358

(22)出願日　平成11年10月29日(1999.10.29)

(31)優先権主張番号　０９／１８２３４２

(32)優先日　平成10年10月29日(1998.10.29)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　599153541
デイタム　インコーポレイテッド
アメリカ合衆国　マサチューセッツ州　ベッドフォード　ミドルセックスターンパイク　54

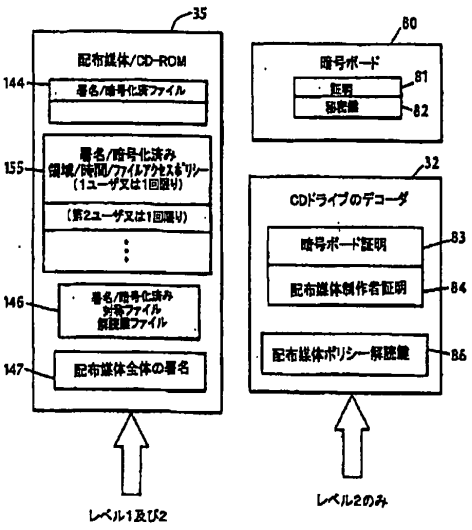
(72)発明者　トーマス　マーク　ヘイスティングス
アメリカ合衆国　マサチューセッツ州　02420　レキシントン　メリアムストリート　38

(74)代理人　100079119
弁理士　藤村　元彦　（外１名）

最終頁に続く

(54)【発明の名称】　格納情報へのアクセス制御

(57)【要約】　（修正有）
【課題】　情報の使用を指定された地理的領域に制限できる格納された情報へのアクセス制御方法。
【解決手段】　ユーザによる格納情報へのアクセスは、実際の地理的位置又は実際の日／時を格納情報へのアクセスが許可された地理的領域又は期間と比較することによって制御される。格納情報が位置する実際の地理的位置及び実際の日／時は、例えば、ＧＰＳ受信機などの信頼できる位置及び時間情報を供給する受信機で受信された信号に基づいて確定される。実際の地理的位置又は日／時が許可された地理的領域又は期間内である場合に格納情報へのアクセスが許可される。受信機から供給される位置及び日／時の情報は、暗号法により署名及び暗号化されてもよい。



【特許請求の範囲】
【請求項１】　格納情報へのアクセスを制御する方法であって、
信頼できる位置情報を供給する受信機で受信した信号に基づいて前記格納情報が位置する実際の地理的位置を確定するステップと、
前記実際の地理的位置を前記格納情報へのアクセスが許可された地理的領域と比較するステップと、
前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。
【請求項２】　請求項１に記載の方法であって、前記受信機はＧＰＳ受信機からなることを特徴とする方法。
【請求項３】　請求項１に記載の方法であって、前記格納情報はコンピュータ可読の媒体に格納されることを特徴とする方法。
【請求項４】　請求項３に記載の方法であって、前記コンピュータ可読の媒体は可撤型であることを特徴とする方法。
【請求項５】　請求項３に記載の方法であって、前記コンピュータ可読の媒体は大容量ディスクからなることを特徴とする方法。
【請求項６】　請求項１に記載の方法であって、前記格納情報は、各々がアクセスが許可される関連した地理的領域を含むファイルからなり、前記実際の地理的位置が前記ファイルの該許可された地理的領域内に位置する場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。
【請求項７】　請求項６に記載の方法であって、前記実際の地理的位置が前記許可された地理的領域に一致しない場合に、前記格納情報へのアクセスを拒否するステップを更に有することを特徴とする方法。
【請求項８】　請求項１に記載の方法であって、
暗号鍵を用いて前記格納情報を暗号化するステップと、
前記実際の地理的位置が前記許可された地理的領域内に位置する場合に、前記格納情報の解読を許す解読キーを提供するステップと、を更に有することを特徴とする方法。
【請求項９】　請求項１に記載の方法であって、
暗号法により前記実際の地理的位置に受信機の暗号鍵で署名するステップと、
実際の地理的位置が前記許可された地理的領域と比較される前に受信機の解読キーで前記受信機の署名を検証するステップと、を更に有することを特徴とする方法。
【請求項１０】　請求項１に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも１つは他のサブセットと異なる許可された地理的領域を有し、該許可された地理的領域が実際の地理的位置内に位置するサブセットへのアクセスは許可され、前記許可された地理的領域が実際の地理的位置内に位置しないサブセットへのアクセスは許可されないことを特徴とする方法。
【請求項１１】　請求項６に記載の方法であって、前記許可された地理的領域との該関連はポリシーファイルとして前記格納情報と共に格納されることを特徴とする方法。
【請求項１２】　格納情報へのアクセスを制御するための装置であって、
信頼できる位置情報を供給して前記格納情報が位置する実際の地理的位置を確定する受信機と、
前記実際の地理的位置を前記格納情報へのアクセスが許可される地理的領域と比較するコンピュータと、を有し、
前記コンピュータは、前記実際の地理的位置が前記許可された地理的領域内に位置する場合に前記格納情報へのアクセスを許すことを特徴とする装置。
【請求項１３】　請求項１２に記載の装置であって、前記受信機はＧＰＳ受信機であることを特徴とする装置。
【請求項１４】　請求項１２に記載の装置であって、前記受信機は、前記実際の地理的位置に暗号法により署名するための受信機暗号鍵を提供する受信機暗号メカニズムを更に有することを特徴とする装置。
【請求項１５】　請求項１４に記載の装置であって、前記格納情報を読み取る読取装置を更に有し、前記読取装置は、該暗号法により署名された実際の位置を検証する受信機解読キーを含むことを特徴とする装置。
【請求項１６】　請求項１５に記載の装置であって、前記読取装置は、前記受信機に送信されて前記実際の地理的位置に加えられる位置オフセットを提供する初期化ベクトルを生成することを特徴とする装置。
【請求項１７】　請求項１６に記載の装置であって、前記位置オフセットに暗号法により署名するための読取装置暗号鍵を提供する読取装置暗号メカニズムを更に有し、前記位置オフセットが前記実際の地理的位置に加えられる前に、該位置オフセット署名は前記受信機によって対応する読取装置解読キーにより検証されることを特徴とする装置。
【請求項１８】　格納情報のより大規模なファイルセットに属するファイルサブセットへのアクセスを制御する方法であって、
該大規模ファイルセットのファイルの各々に一意のファイル暗号鍵を関連付けて、該関連暗号鍵を用いて前記ファイルを暗号化するステップと、
前記格納情報へのアクセスが許可される少なくとも１つの許可された地理的領域を前記大規模ファイルセットのファイルの各々に関連付けるステップと、
信頼できる位置情報を供給する受信機で受信された信号に基づいて、前記格納情報が位置する実際の地理的位置を確定するステップと、
前記実際の地理的位置を前記許可された地理的領域と比

較するステップと、
実際の地理的位置が前記ファイルサブセットに属するファイルの前記許可された地理的領域内に位置する場合に、前記ファイルサブセットに属する前記ファイルへのアクセスを許可し解読を許すファイル解読キーを供給するステップと、を有することを特徴とする方法。
【請求項１９】　請求項１８に記載の方法であって、前記ファイルと前記許可された地理的領域との前記関連はポリシーファイルを含むポリシーとして格納され、前記ポリシーファイルの各々は、ユーザ・パスワードによりアクセスでき、実際の地理的位置が前記ファイルに関連した前記許可された地理的領域内に位置しユーザ・パスワードが有効な場合に前記ポリシーファイルにリストされたファイルへのアクセスを許可することを特徴とする方法。
【請求項２０】　請求項１９に記載の方法であって、前記ポリシーは前記格納情報と共に格納されることを特徴とする方法。
【請求項２１】　格納情報へのアクセスを制御する方法であって、
信頼できる時間情報を供給する受信機で受信された信号に基づいて前記格納情報の位置における実際の日付又は時間を確定するステップと、
前記実際の日付又は時間を前記格納情報へのアクセスが許可される所定の日付又は時間の期間と比較するステップと、
前記実際の日付又は時間が該許可された日付又は時間の期間内に発生した場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。
【請求項２２】　請求項２１に記載の方法であって、前記実際の日付又は時間が前記許可された日付又は時間の期間内に発生しなかった場合に前記格納情報へのアクセスを拒否するステップ、を更に有することを特徴とする方法。
【請求項２３】　請求項２１に記載の方法であって、前記情報は、各々がアクセスが許される関連した許可された日付又は時間の期間を有するファイルを有し、前記実際の日付又は時間が該関連した許可された日付又は時間の期間内に発生した場合に前記ファイルへのアクセスを許すステップを更に有することを特徴とする方法。
【請求項２４】　請求項２１に記載の方法であって、前記格納情報は情報のサブセットに分割され、前記サブセットの少なくとも１つは他のサブセットと異なる許可された日付又は時間の期間を有し、前記実際の日付又は時間に一致する許可された日付又は時間の期間を有するサブセットへのアクセスは許可され、前記実際の日付又は時間に一致しないサブセットへのアクセスは許可されないことを特徴とする方法。
【請求項２５】　格納された情報へのアクセスを制御する方法であって、
前記情報を許可された地理的領域及び許可された期間と関連付けたポリシーを形成するステップと、
暗号法により前記ポリシー及び前記情報に署名を行うステップと、
該署名されたポリシーを該署名された情報と共に格納するステップと、
前記ポリシーのロックを解除するパスワードを供給するステップと、
信頼できる位置情報を供給する受信機で受信された信号に基づいて、該格納された情報が位置する実際の地理的位置を確定するステップと、
実際の時間を確定するステップと、
前記実際の地理的位置及び前記実際の時間を前記ポリシーの前記許可された地理的領域及び前記許可された期間と比較するステップと、
前記実際の地理的位置及び前記実際の時間が前記ポリシーの前記許可された地理的領域及び前記許可された期間内である場合に前記格納情報へのアクセスを許すステップと、を有することを特徴とする方法。
【請求項２６】　請求項１に記載の方法であって、前記信頼できる位置及び時間の供給源は全地球周回ナビゲーション衛星システムであることを特徴とする方法。
【請求項２７】　請求項１に記載の方法であって、前記信頼できる位置及び時間の供給源は慣性航法システムであることを特徴とする方法。
【請求項２８】　請求項１に記載の方法であって、前記信頼できる位置及び時間の供給源は衛星ベースの位置確定システムであることを特徴とする方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、格納された情報へのアクセス制御に関する。
【０００２】
【従来の技術】例えばＣＤ－ＲＯＭ等のデータ配布媒体には多数のファイルを格納することができる。ＣＤ－ＲＯＭの製作者は、秘密扱いである、又はユーザによる支払いを要するという理由から特定のファイルへのユーザのアクセスを制御することを望む場合がある。
【０００３】ユーザに対しＣＤ－ＲＯＭ製作者から得られるパスワードの入力を要求することによってアクセスを制御してもよい。異なるパスワードによって、異なるファイル又は異なるファイルのサブセットのロックが解除（アンロック）されてもよい。ファイルは、暗号によって署名され、更に保護のために暗号化されてもよい。製作者がその製作者だけが知っている一意の鍵（キー）によって各ファイルを暗号化する方法について記載された米国特許第5,646,992号を参考文献としてここに挙げる。ユーザが暗号化されたアイテムを受け取り、製作者がそのユーザのアクセス要求を処理した後、ユーザは暗号化された各ファイルの解読に用いられる解読鍵（すな

わち、パスワード）を受け取る。パスワードは、アクセスが要求されたファイルのみロックを解除する。

【０００４】

【発明の概要】本発明は、信頼できる位置情報を供給する受信機により受信した信号に基づいて配置される格納情報の実際の地理的位置を確定することによって格納情報へのアクセスを制御することを一つの特徴としている。次に、実際の地理的位置は、格納情報に対するアクセスが許可される地理的な領域と比較される。実際の地理的位置が許可された地理的領域内に位置する場合、ユーザは格納情報へのアクセスを許される。

【０００５】本発明の実施例は、以下の特徴を含んでいる。位置情報を供給する受信機は、衛星ベースの位置確定システム又は慣性航法装置から位置情報を受信することができる。その情報は、コンピュータ可読の媒体（例えば、大容量ディスク）に格納される。格納情報はファイルを含み、これらのファイルの各々はアクセスが許される関連した地理的領域を含む。実際の地理的位置がファイルに許可された地理的領域内に位置する場合、ユーザはその特定のファイルにアクセスできる。格納情報は暗号化することができ、実際の地理的位置が許可された地理的領域内に位置する場合だけ、ユーザは解読鍵にアクセスできる。また、格納情報は情報のサブセットに分割することができ、少なくとも１つのサブセットは他のサブセットとは異なる許可領域を有する。許可された地理的領域とファイルとの対応は、ポリシーファイル（policy file）として格納情報と共に格納される。

【０００６】本発明は他の特徴として、信頼できる時間情報を供給する受信機により受信された信号に基づいて格納情報の位置における実際の日付又は時間を確定する。実際の日付又は時間は、格納情報に対するアクセスが許可された所定の日付又は時間の期間と比較される。実際の日付又は時間が許可された期間内にある場合、ユーザは格納情報にアクセスすることができる。

【０００７】本発明は他の特徴として、格納情報が位置する実際の地理的位置を確定するために信頼できる位置情報を供給する受信機を含む。コンピュータは、格納情報へのアクセスが許可される地理的領域と位置情報を受信し、実際の地理的位置が許可された地理的領域内に位置する場合にアクセスを許可する。本発明の実施例は以下の特徴を有している。受信機は、暗号法により実際の地理的位置に受信機暗号鍵で署名して、実際の地理的位置が許可された地理的領域と比較される前に、その受信機署名を受信機解読鍵で検証する受信機暗号メカニズムを含む。

【０００８】更に他の特徴として、本発明は、暗号によって署名された実際の位置を検証するための対応する受信機解読鍵を有する読取装置を含む。本発明の実施例は、以下の特徴を含む。読取装置は、受信機に送信されて実際の地理的位置に加えられる位置オフセットを提供する初期化ベクトルを生成する。読取装置は、読取装置暗号鍵によって位置オフセットに暗号署名する。受信機は、位置オフセットが実際の地理的位置に加えられる前に、対応する読取装置解読鍵により位置オフセットの署名を検証する。

【０００９】本発明の他の特徴として、情報と許可された地理的領域及び許可された期間とを関連させるポリシーを形成し、暗号によってその情報及びポリシーに署名する。署名されたポリシーは、署名された情報と共に格納される。ユーザは、実際の地理的位置及び実際の時間がそれぞれ許可された地理的領域及び許可された期間内にある場合に、製作者からポリシーのロックを解くためのパスワードを得て、格納情報にアクセスすることができる。

【００１０】本発明の利点について以下に述べる。格納情報の製作者は、その情報の使用を指定された地理的領域に制限するか、又は使用が許されない指定領域を除外することができる。例えば、ＣＤ－ＲＯＭに格納される自動車のサービス・マニュアルは、対応する特定の国及び／又は領域に適用できる異なるセクションの情報を含んでいてもよい。ユーザは、現在の地理的位置に適用できる一部の情報のみを見ることが許されてもよい。同様に、機密に関わる会社のレポートへのアクセスは、特定の施設位置に限られていてもよい。時間に敏感な情報に対するアクセスは、一定の日の前又は後に拒否されるか、又は許された期間に限られてもよい。許可された地理的領域及び期間についての情報を、ＣＤ－ＲＯＭに格納されユーザ・パスワードによってアクセスされるポリシー・ファイルと関連させることによって、ＣＤ－ＲＯＭの製作者は、ユーザが特定のポリシー・ファイルの一式、従って、対応する領域及び日／時間で許可された情報にアクセスすることを許可する新たなパスワードを発行することができる。

【００１１】本発明の他の利点及び特徴は、下記の記載及び特許請求の範囲から明らかになる。

【００１２】

【発明の実施の形態】図１ないし図３に示すように、データ配布媒体３５として用いられる携帯用のコンピュータ可読のＣＤ－ＲＯＭに格納された情報へのアクセスは、情報へのアクセスがなされるコンピュータ・システム１０の実際の地理的位置及びアクセスされる時間に基づいて制御されてもよい。

【００１３】コンピュータ・システム１０において、コンピュータ２０はキーボード５０、マウス６０、モニター４０及びＣＤ－ＲＯＭドライブ３０に接続されている。ＧＰＳ受信機７０は、信頼できる位置情報及び時間情報の供給源として機能する。受信機７０は、コンピュータ・システム１０の実際の地理的位置に位置し、周回するＧＰＳ衛星９０（１つのみを示す）から信号７５を受信する。受信機７０は、受信信号７５を経度、緯度及

び高度について数メートルの精度の地理的位置データ７１、及びマイクロ秒の精度の日／時データ７１に変換する。データ７１は、デバイス・ドライバ７２を経てコンピュータ２０に送信される。

【００１４】図６に示すように、受信機暗号ボード８０は、製作者よって署名された公開鍵証明書８１及び対応する秘密鍵８２を含んでもよい。また、地理的位置及び日／時データ７１は、データを認証するために秘密鍵８２によって署名されてもよい。また、図６に示すように、ＣＤ－ＲＯＭドライブ３０は、ハードウェア又はソフトウェアとして組み込まれた暗号及び署名機能（デコーダ３２）を含んでもよい。デコーダ３２は、証明書８１と同一の暗号ボード公開鍵証明書８３、製作者の身元確認のための製作者証明８４、及びその製作者によって署名された配布媒体ポリシー解読鍵８６を含む。暗号ボード証明８３は、秘密鍵８２によって署名された暗号ボード８０の署名を検証する。ポリシー解読鍵８６は、ＣＤ－ＲＯＭ３５に格納されたアクセス・ポリシー１５５を解読する。

【００１５】下記の実施例に記載するように、コンピュータ・システム１０は、レベル１及びレベル２等の数レベルのセキュリティを有することができる。レベル１のセキュリティを有するシステムにおいて、受信機７０は従来のデバイス・ドライバ７２を介してコンピュータ２０と通信する。また、ＣＤ－ＲＯＭドライブ３０は従来のＣＤ－ＲＯＭである。受信機７０及びＣＤ－ＲＯＭドライブ３０は、付属の暗号／解読機能を有していない。セキュリティを高めるため、レベル１のシステムのコンピュータ２０は、データを認証及び／又は暗号化することができる「信頼できる」コンピュータである。さらに安全のため、レベル２のシステムにおいては、受信機７０は暗号ボード８０を含み、ＣＤ－ＲＯＭドライブ３０はデコーダ３２を含んでもよい。レベル２のシステムは、データ認証、及び受信機７０とデコーダ３２との間のデータ伝送の暗号化を行うように設計される。また、コンピュータ２０は、データ認証及び暗号化を行わない市販のコンピュータであってもよい。

【００１６】キーボード５０及びマウス６０からの入力データは、ユーザ・インタフェース９５を介して入力された通常のコマンド及びデータ入力１３０（アプリケーション・プログラム３４によって提供される）、及びユーザがデータ配布媒体３５に格納された情報にアクセスするための一つ以上のパスワード１３０を含んでもよい。

【００１７】ＣＤ－ＲＯＭ３５は、情報ファイル１４４、許可された地理的領域のリスト１５０、許可された日／時の期間のリスト１５４、一つ以上のファイル解読鍵ファイル１４６、一つ以上のポリシー・ファイル１５２及びＣＤ－ＲＯＭ３５全体の署名１４７等の種々の情報を格納する。図３に示すように、ファイル１４４、１４６、１５０、１５２、１５４及び１５５は署名及び暗号化されてもよい。

【００１８】ファイル１４４は、サブセット１４１、１４２及び１４３にグループ化されてもよい。また、ファイルは複数のサブセットに属していてもよい。（以下の説明において、ファイルの語は、ファイル及びファイル・サブセットの両者を意味する）。ファイル１４１、１４２及び１４３のそれぞれは、一意的なファイル暗号鍵５１（Ｅ１、Ｅ２、Ｅ３）によって暗号化されてもよい。対応するファイル解読鍵５２（Ｋ１、Ｋ２、Ｋ３）は、ＣＤ－ＲＯＭ３５のファイル解読鍵ファイル１４６に格納される。解読鍵及び解読鍵ファイルに関する更なる情報は、米国特許第5,646,992号に記載されている。

【００１９】ＣＤ－ＲＯＭ３５上のファイル１４１、１４２及び１４３の各々は、許可された地理的領域のリスト１５０に格納された許可された地理的領域のうちゼロ又は１つ以上と関連付けられている。例えば、ニューヨーク市のエンパイアステートビルの範囲に対応する緯度及び経度、及び５０ないし６０メートルの高度で領域が区切られ、その領域に関連するファイルは、受信機７０がエンパイアステートビルの一定のオフィス領域内に位置する場合にのみ開くことができる。

【００２０】同様に、ファイル１４１、１４２及び１４３の各々は、許可された日／時の期間のリスト１５４に格納された許可された期間のうちゼロ又は１つ以上と関連付けらる。ＧＰＳ衛星９０のそれぞれは、極めて高精度のクロックを維持する。受信機７０は信号７５の一部としてＧＰＳクロック信号を受信するか、又は、ローカルな原子時計が同様のクロック信号を提供する。情報へのアクセスが試みられているときに、クロック信号によって実際の時間に基づいた情報へのアクセスが制御可能になる。例えば、製作者は、（１）所定の日／時の前、（２）所定の日／時の後、又は、（３）所定の日／時の期間の間だけアクセスが許されるように指定することができる。

【００２１】ユーザがキーボード５０から入力するパスワード１３０によって、製作者はファイル１４１、１４２及び１４３とリスト１５０及び１５４の特定のアイテムとを関連付けることができる。パスワード１３０は、複数のアクセスに有効なユーザ・パスワード、又は１回限りのパスワードであってもよい。または、製作者は、ポリシー・ファイル１５２によってリスト１５０及び１５４の特定の地理的領域／日／時の情報とファイル１４１、１４２及び１４３とを関連付けることができる。有効なユーザ・パスワード１３０は、一つ以上のポリシー・ファイル１５２のロックを解除するものであってもよい。ユーザの実際の地理的位置及び現在の日付及び時間がユーザ・パスワード１５０に対応する許可された地理的領域及び許可された日／時内である場合、ユーザはユーザ・インタフェース９５を介して選択したファイルに

アクセスすることができる。次に、選択された情報は出力装置４０上に表示される。

【００２２】表１は、１例として、ＣＤ－ＲＯＭ３５に格納され、対応する許可された地理的領域及び日／時と関連付けられた５つの暗号化済みファイルＡないしＦにどのようにアクセスすることができるかを示している。各ファイルは、４つの異なるファイル解読鍵Ｋ１ないしＫ４のうちの１つと関連付けられている。Ｌ１及びＬ２は２つの異なる許可された地理的領域であり、Ｔ１、Ｔ２及びＴ３は３つの異なる許可された日／時の期間である。ファイル解読鍵Ｋ１（例えば、パスワード）を所有するユーザは、時刻Ｔ１において地理的領域Ｌ１及びＬ３内のマニュアルＡを解読することができる。同じユーザは、また、領域Ｌ２及びＬ３内で同一の時刻Ｔ１においてマニュアルＤを解読することができるが、領域Ｌ１内では解読できない。同様に、鍵Ｋ２を有するユーザは、領域Ｌ２内で画像Ｂ及び画像Ｅを解読できるが、同じ時刻では解読できない。図面Ｃは、時刻Ｔ３ではいかなる位置においても解読することができるが、業務報告書Ｆは鍵Ｋ４を必要とし、領域Ｌ１内であればいつでも解読することができる。

【００２３】

【表１】

暗号化されたファイル	ファイル解読鍵	許可された地理的領域	許可された日/時の期間
マニュアルA	K1	L1, L3	T1
画像B	K2	L2	T1, T3
図面C	K3	--	T3
マニュアルD	K1	L2, L3	T1
画像E	K2	L2	T2
報告書F	K4	L1	--

図３に示すように、任意の暗号による暗号署名のために、製作者はＣＤ－ＲＯＭ３５に書くべきソース・ファイル１４４’を選択し、許可された地理的領域１５０’のリスト及び許可された日時の期間１５４’のリストを指定する。製作者は、各ファイル又はファイル・サブセットをゼロ又は１つ以上の地理的領域１５０’、及びゼロ又は１つ以上の日時の期間１５４’と関連付けて（表１参照）、この関連付けをポリシーファイル１５２’に格納する。ファイル１４４’、１５０’、１５２’、１５４’の各々は、ステップ５３、３４０、３５０及び３６０において対応する暗号鍵５１、３４５、３５５及び３６５によって署名、暗号化される。対応する暗号化されたファイル１５０、１５２及び１５４は、署名、暗号化された領域／時間／ファイルアクセス・ポリシー１５５として格納される。上述した如く、署名／暗号化されたファイル１４４、署名／暗号化された対称ファイル解読キーファイル１４６、及び製作者がＣＤ－ＲＯＭ３５全体に署名するために用いられる署名１４７もまたＣＤ－ＲＯＭ３５に格納される。

【００２４】図４及び図５に示すように、署名／暗号化ファイル１４４にアクセスするために、ユーザは製作者からパスワード１３０（図２）を得て（ステップ４００）、キーボード５０からパスワード１３０を入力する（ステップ４１０）。パスワード１３０は１回限りの（ワンタイム）パスワードであると仮定される。但し、複数のセッションに有効なユーザ・パスワードを用いることもできる。

【００２５】図４に示すように、レベル１及びレベル２に関するプロセス・フローの初期の部分はほとんど同一である。ステップ４２０においてパスワード１３０をチェックし、システム構成に従い、ステップ４４０（レベル１の場合、追加のセキュリティなし）又はステップ４５０（レベル２の場合、受信機／ＣＤ－ＲＯＭドライブのセキュリティ有り）を実行する。図５に示されるステップ４４０及びステップ４５０の詳細について以下に説明する。

【００２６】図５に示すように、プロセス４４０において、ユーザのパスワード１３０はデバイス・ドライバ７２に送られる（ステップ５１０）。デバイス・ドライバ７２は、ワンタイム・パスワード１３０に応答して、それ自身のワンタイム・パスワードをユーザ・パスワード１３０から生成し（ステップ５２０）、ユーザが実際に正しいワンタイム・パスワード１３０を入力したことを検証し（ステップ５３０）、ユーザにインタラクティブ・セッションを認証する（ステップ５３２）。さもなければ、アクセスは拒否される（ステップ５３５）。

【００２７】一度、パスワード１３０によってユーザが認証されると、デバイス・ドライバ７２は現在の位置及び日／時を受信機７０に問い合わせる（ステップ５４０）。次に、デバイス・ドライバ７２は、受信機７０から戻された時間及び位置データと、ファイル１４４又はファイル・サブセット１４１、１４２及び１４３に適用

するポリシー１５５を比較する（ステップ４６０）。ユーザがファイル１４４へのアクセスを許可されると、次に、データは解読鍵５２によってロックが解かれて（ステップ４７０、図３）解読され（ステップ４８０）、ユーザのアプリケーション・プログラム３４に供給され表示される（ステップ４９０）。

【００２８】レベル２のシステムにおいて、受信機７０は、以下において「暗号ボード」と称される暗号の受信機ボード８０を含む。前述のように、暗号ボード８０はメッセージの署名及び暗号化／解読を行うことができる。ＣＤ－ＲＯＭドライブ３０は、暗号ボード８０により署名され暗号ボード８０から受信される位置データを復号するためのデコーダ３２を含む。

【００２９】図５に示すように、プロセス４５０において、ユーザ・パスワード１３０は、パスワード１３０を受付けそれを変更せずにデコーダ３２に渡すデバイス・ドライバ７２に送られる（ステップ５５０）。次に、ドライバ３２は、ユーザ・パスワードに対応するそれ自身のワンタイム・パスワードを秘密鍵８６によって内部で生成し（ステップ５６０）、正しいパスワード１３０がデバイス・ドライバ７２に送信されたことを検証し（ステップ５７０）、ユーザにインタラクティブ・セッションを認証する（ステップ５７２）。さもなければ、アクセスは拒否される（ステップ５７５）。

【００３０】一度、暗号回路３２がユーザを認証すると、ドライバ３２はデバイス・ドライバ７２を介して暗号ボード８０に受信機７０からの現在の時刻及び位置情報について問い合わせる（ステップ５８０）。デコーダ装置３０は、暗号ボード８０に「初期化ベクトル」、すなわち、デバイス・ドライバ７２が時間及び位置についての要求とともに暗号ボード８０に渡す位置オフセットを形成する（ステップ５９０）ための署名されたランダム又は他のビット・パターンを供給する（ステップ５９０）。

【００３１】暗号ボード８０は、現在の時刻及び緯度、経度、高度による実際の地理的位置を含む予め確立されたデータ・フォーマットに応じたパケットを準備することによって応答する（ステップ６００）。また、計算に必要な他のデータと同様に位置データを送信する衛星の識別情報が含まれていてもよい。暗号ボード８０は、また、供給された初期化ベクトルをパケット内に既知のオフセットで格納し、パケット内容に暗号署名を適用する。暗号の署名は、例えば、メッセージ・ダイジェスト／パケット・データの寄せ集め（ハッシュ）、さらにある所定鍵によるメッセージ・ダイジェストの暗号であってもよく、あるいは暗号ボード８０に格納された証明又は鍵に応じて対称又は非対称であってもよい。

【００３２】次に、暗号ボード８０は、パケットをデコーダ３２／ＣＤ－ＲＯＭドライブ３０に中継するデバイス・ドライバ７２に署名された時間／位置パケットを送信する（ステップ６０５）。デコーダ３２は、暗号ボード８０から受信したパケットの署名をデコーダ３２に格納された署名と比較する（ステップ６１０）。その署名が適切に検証されると（ステップ６２０）、パケット内の初期化ベクトルが調べられ、ステップ５９０においてデコーダ３２が暗号ボード８０に実際に供給した初期化ベクトルと同一の初期化ベクトルであるかを確定する。これが本当ならば、デコーダ３２が受信したパケットは最近のもので真性なものであり、時間及び位置データは有効であるとして受け付けられる。

【００３３】一度、暗号ボード８０からのパケットが署名及び初期化ベクトルに基づいて許可されると、デコーダ３２は、暗号ボード８０から受信した時間及び位置データをファイル１４４又はファイル・サブセット１４４に適用されるポリシー１５５と比較する（ステップ４６０）。ユーザがファイル１４４へアクセスすることが許可されると、データのロックは解かれ（ステップ４７０）、解読鍵５２により解読されて（ステップ４８０）、ユーザ・アプリケーション・プログラム３４に供給され表示される（ステップ４９０）。

【００３４】他の実施例は、特許請求の範囲内である。例えば、ＧＰＳ受信機は正確にデータ配布媒体読取装置の位置に配置されている必要はなく、読取装置に対して既知の位置（例えば、建物のローカルエリア・ネットワークにコンピュータ・サービスを提供するコントロール・サーバを含む部屋など）に配置されていればよい。また、ポリシー・ファイル１５２'は、一定のファイル１４４に対するアクセスが拒否される地理的領域を指定してもよい。

【００３５】ファイルに対するアクセスの制限は、製作者によりキーボードから入力されるパスワードに限定されない。例えば、顔の特徴、指紋及び／又は声紋などの一定の生物測定学的属性をパスワードに加えて、又はパスワードの代りに用いてもよい。

【図面の簡単な説明】

【図１】コンピュータ・システムの斜視図である。

【図２】格納情報へのクセスを制御するコンピュータベースのシステムのブロック図である。

【図３】フローチャートである。

【図４】フローチャートである。

【図５】フローチャートである。

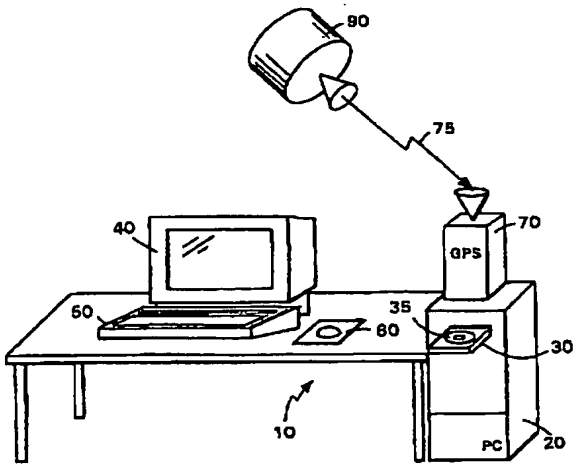
【図６】暗号の構成要素を示すブロック図である。

【主要部分の符号の説明】

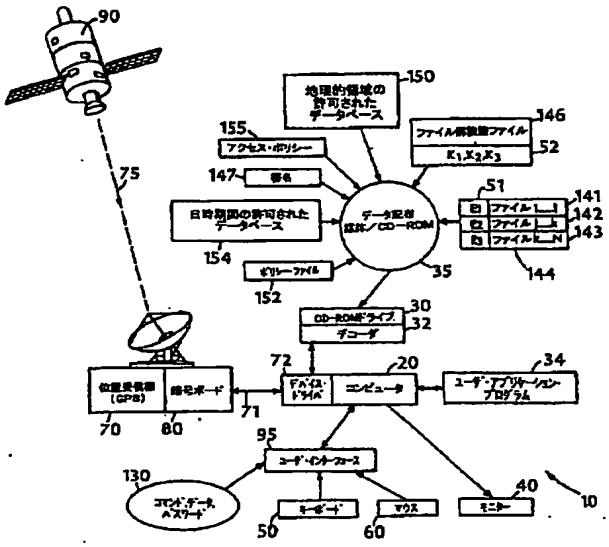
１０　コンピュータ・システム
２０　コンピュータ
３２　デコーダ
３５　データ配布媒体
７０　ＧＰＳ受信機
８０　暗号ボード
８１　証明書

８２　秘密鍵
８３　暗号ボード公開鍵証明
８４　製作者証明
８６　配布媒体ポリシー解読鍵
９０　ＧＰＳ衛星
１４４　情報ファイル
１４６　ファイル解読鍵ファイル
１４７　配布媒体の署名
１５５　アクセス・ポリシー

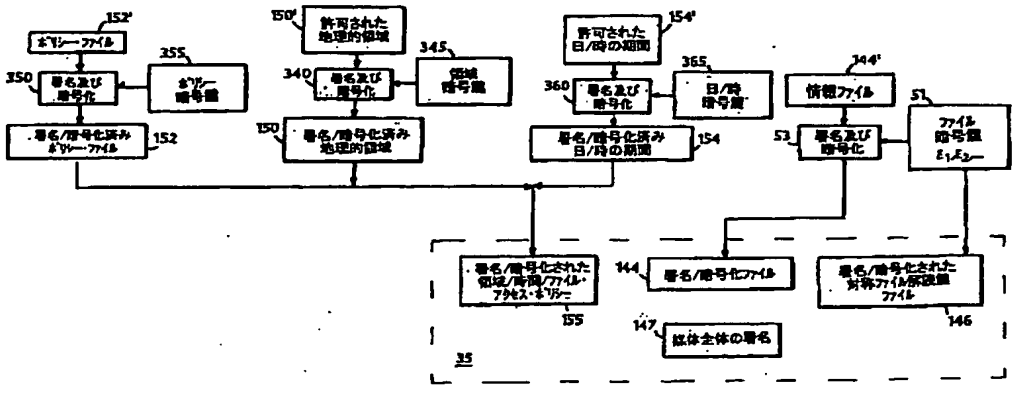
【図１】



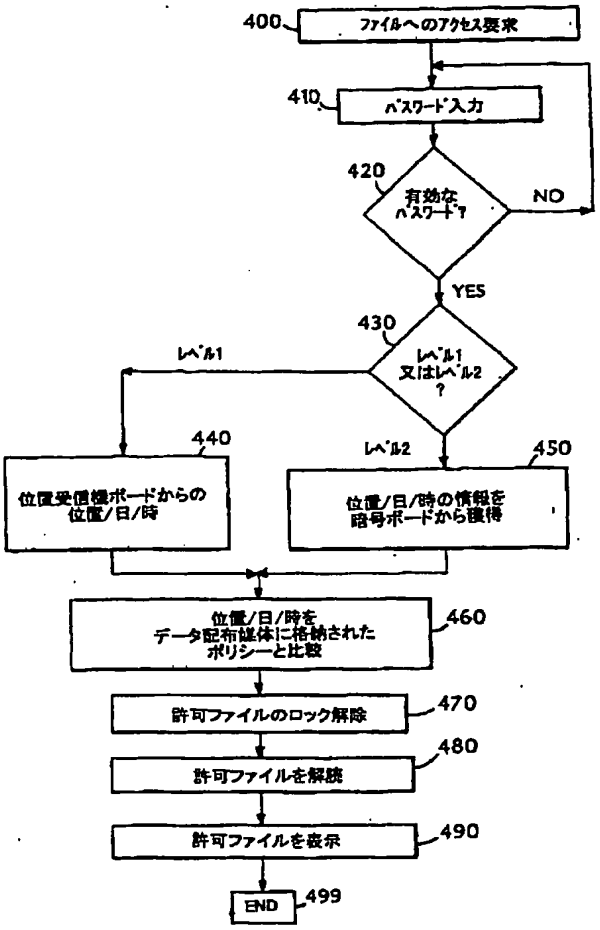
【図２】



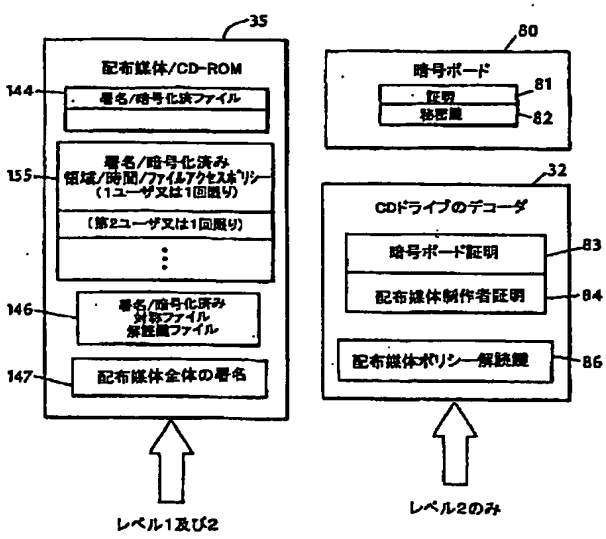
【図３】



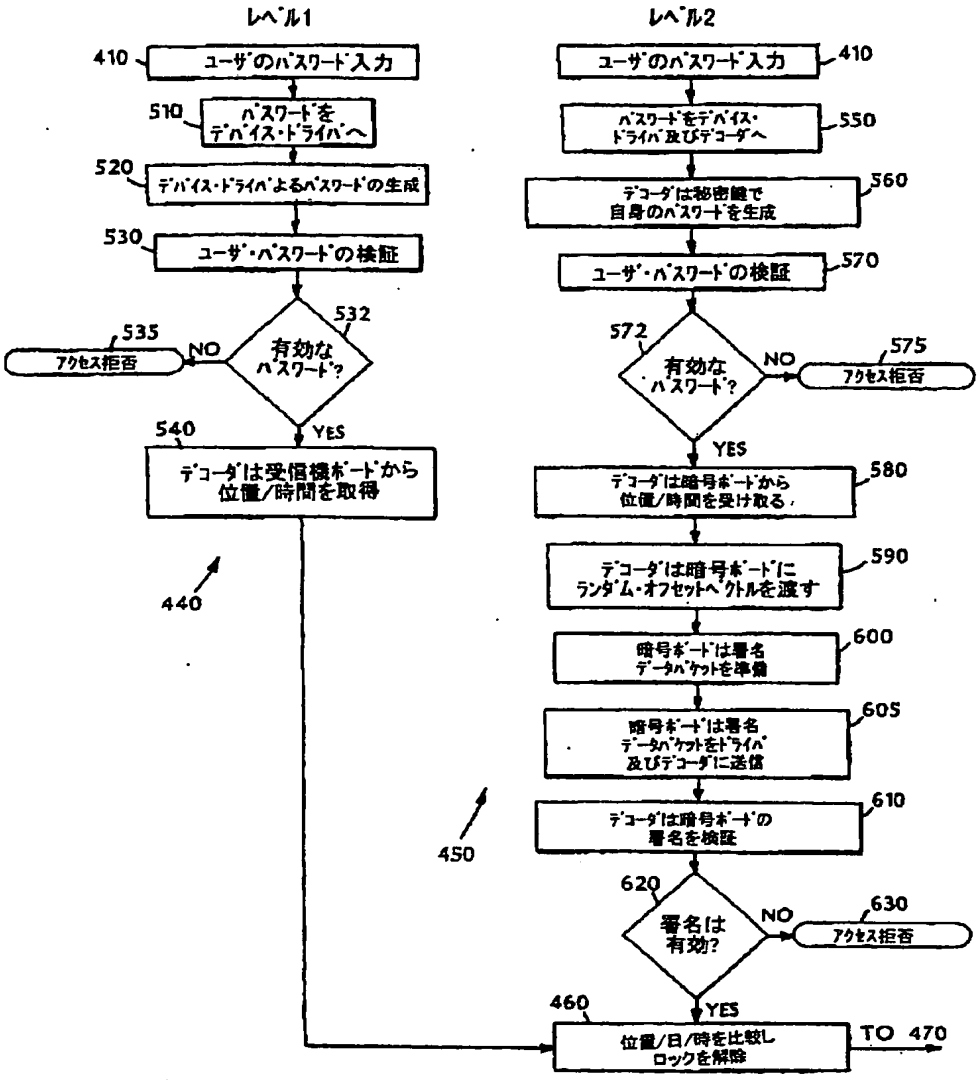
【図４】


400
ファイルへのアクセス要求
410
パスワード入力
420
有効なパスワード?
NO
YES
430
レベル1又はレベル2?
レベル1
レベル2
440
位置受信機ボードからの位置/日/時
450
位置/日/時の情報を暗号ボードから獲得
位置/日/時をデータ配布媒体に格納されたポリシーと比較
460
許可ファイルのロック解除
470
許可ファイルを解読
480
許可ファイルを表示
490
END
499

【図６】


35
配布媒体/CD-ROM
144
署名/暗号化済ファイル
155
署名/暗号化済み領域/時間/ファイルアクセスポリシー(1ユーザ又は1回限り)
(第2ユーザ又は1回限り)
146
署名/暗号化済み対称ファイル解読鍵ファイル
147
配布媒体全体の署名
レベル1及び2
80
暗号ボード
81
証明
82
秘密鍵
32
CDドライブのデコーダ
83
暗号ボード証明
84
配布媒体制作者証明
86
配布媒体ポリシー解読鍵
レベル2のみ

【図５】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	ﾃｰﾏｺｰﾄﾞ (参考)
Ｈ０４Ｌ 9/14		Ｈ０４Ｌ 9/00	６４１

(72) 発明者 マイケル イー. マックニール
アメリカ合衆国 カリフォルニア州 95018 フェルトン ロストエイカードライブ 1271

(72) 発明者 トッド エス. グラッシィ
アメリカ合衆国 カリフォルニア州 95066 スコッツバリー ブルーボネットレーン 109エイ

(72)発明者　ジェラルド　エル.　ウィレット
アメリカ合衆国　マサチューセッツ州
02148　マルデン＃１　ハーバードストリート　189